CRYPT-02

To hide passwords, always use with a random salt for each hash

Sean Barnum, Cigital, Inc. [vita[1]]

2007-03-22

Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 3822 bytes

Attack Category	• Encryption Assault
Vulnerability Category	• Cryptography
Software Context	• Cryptography
Location	
Description	If crypt() must be used to hide passwords, it should be used with a random salt for each hash. The crypt() function should be avoided in favor of stronger hash functions. However, if crypt() must be used, it should never be used in the form crypt(pwd, pwd), where the password is also being used as the salt. This is because the first two bytes of the salt will always be prepended to the hash and will be visible in plaintext. Hence, using the password as the salt reveals two characters of the password. This leaves only 6 characters of "secret information," which would require a dictionary of size less than 2^40 to crack. Also, if the same salt is used for all passwords, then once an attacker knows the salt, his or her work is reduced to the same amount as when no salt was present.
APIs	**Function Name** / **Comments** crypt / look for crypt(x, x) with same param twice
Method of Attack	
Exception Criteria	
Solutions	**Solution Applicability** / **Solution Description** / **Solution Efficacy** When one must use crypt() / The ideal solution is to use a more secure routine provided by a cryptographic library. If this / Somewhat effective. Use of a more secure hash algorithm would be preferable.

1. http://buildsecurityin.us-cert.gov/bsi-rules/35-BSI.html (Barnum, Sean)

		is not possible, ensure that the salt changes with each password and that it cannot be computed using the password. The salt and the password must be completely independent of each other.	

Signature Details	char *crypt(const char *pwd, const char *pwd)
Examples of Incorrect Code	`hash = crypt(password, password);`
Examples of Corrected Code	`salt = get_random_salt(); /* See McGraw et al. p. 345 for a sample implementation of this function. */` `hash = crypt(password, salt);`
Source Reference	Viega, John & McGraw, Gary. Building Secure Software: *How to Avoid Security Problems the Right Way*. Boston, MA: Addison-Wesley Professional, 2001, ISBN: 020172152X, pp. 337+. This is a good description of crypt().
Recommended Resource	
Discriminant Set	**Operating Systems**: • UNIX (All) • Windows **Languages**: • C • C++

Cigital, Inc. Copyright

1. mailto:copyright@cigital.com